Comments Submitted to the Federal Communications Commission

Customer Proprietary Network Information (CPNI)
CC Docket No. 96-115

Submitted by
Privacy Rights Clearinghouse
Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumers Union
National Consumers League
PrivacyActivism
Utility Consumers' Action Network

April 14, 2006

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
Filed electronically: www.fcc.gov/cgb/ecfs

RE: Customer Proprietary Network Information (CPNI) – CC Docket No. 96-115

Dear Secretary Dortch:

The Privacy Rights Clearinghouse (PRC) and the following organizations[1] take this opportunity to comment on the need to safeguard the telephone calling records of customers, known as "customer proprietary network information" or CPNI:

Consumer Action
Consumer Federation of America
Consumer Federation of California
Consumers Union
National Consumers League
PrivacyActivism
Utility Consumers' Action Network

These nonprofit consumer organizations represent the interests of millions of telephone consumers throughout the nation. (See Endnotes for descriptions of organizations.)

Our comments respond to the Federal Communications Commission's (FCC or Commission) proposed rule published on March 15, 2006, and concurrent order granting the Petition for Rulemaking of the Electronic Privacy Information Center (EPIC).[2]

1. Introduction
2. The Need for Stringent Carrier Safeguards
3. EPIC's Proposed Security Measures
4. Existing Opt-Out Regime for Joint Partners
5. Conclusion

1. Introduction

Consumers expect that their telephone calling records will remain private and unavailable to third parties without the customer's knowledge and authorization. Yet, it is clear that this expectation is unrealistic, evidenced by the findings in the Petition for Rulemaking submitted to the Commission by the Electronic Privacy Information Center (EPIC).[3]

EPIC's Petition as well as recent news reports, state and federal legislative proposals, and government lawsuits against data brokers all point to a disturbing situation: Not only are current safeguards for customer calling records inadequate, but those that exist are being blatantly ignored.

As the Commission notes and as illustrated by EPIC's Petition, numerous web sites advertise the sale of personal telephone records. For a price, an individual's complete calling history can be revealed. Even the location of a cell phone can be tracked. This is not only a misuse of private information, but it is also illegal. And for some individuals, such access can be life threatening – for example, victims of domestic violence and stalking.

Sale of phone records by online data brokers is by all accounts a thriving market. The number of web sites that advertise the sale of phone records suggest that CPNI is readily available from carrier records and does not result from the isolated activities of a few bad actors.

A two-pronged approach is needed to halt this flow of customers' personal data. First, those who obtain CPNI through illegal means should be stopped. Second, the Commission should adopt stringent security measures and financial incentives to prevent the flow of personal information from the carriers to the data vendors.

We are encouraged by the Commission's NPRM and grant of EPIC's Petition. The Commission's attention is a much-needed first step toward protecting consumer privacy. We trust that this signals the Commission's commitment to quickly adopt and enforce more stringent carrier safeguards for CPNI.

The Commission proposal seeks comment, among other things, on how data brokers are able to obtain CPNI. This fact-finding effort will likely result in many comments from carriers and others, which could take considerable time for the Commission to analyze. If so, the Commission should consider adopting temporary emergency security measures to immediately stop the flow of personal data from carriers.

2. The Need for Stringent Carrier Safeguards

Efforts must be undertaken to stop pretexting, hacking, and other means by which data brokers and others gain unauthorized access to personal phone accounts. The fact that there are many web sites offering phone records for sale is an indication that current safeguards are inadequate and that carriers need to do more.

The Federal Trade Commission (FTC) reports that it is currently investigating data brokers that obtain and sell customer phone records.[4] The agency says it will focus its efforts on pretexting, that is obtaining information under false pretenses, to stop the sale of sensitive telephone records over the Internet. The FTC's investigation is welcome news for consumers. However, it is likely not enough to stop individual data brokers. After all, by whatever means, data brokers appear to be unfettered in obtaining their "product" from carriers.

In reviewing comments from carriers, the Commission may well hear that the problem lies, not with inadequate carrier security, but with those who abuse the system by illegally accessing CPNI. The challenges inherent in directing enforcement efforts solely at those who illegally access customer records was illustrated in a recent case filed by the California Attorney General against the web site Data Trace USA, www.datatraceusa.com, and the site operator Ilia S. Nichols. Investigators from the agency used an alias and credit card to order the cell phone records of a deputy attorney general from Data Trace. Employees of the data broker, posing as the phone customer, accessed the Verizon Wireless web site and created an online account through which they obtained the phone records, which showed not only a list of calls but when the calls were placed and how long they lasted. Data Trace sold that information to the undercover investigators for $220.

The Data Trace site no longer operates. The company, incorporated in Florida, at last report could not be located to effect service of the California lawsuit. The operator of the site, according to the California lawsuit, uses a number of aliases.[5] There is nothing to stop this or any other fly-by-night vendor from setting up shop again, incorporating under another name or in another state, and using a different alias. The best strategy to stop illegal access of this sort is to adopt more stringent carrier security measures.

In addition to adopting stronger carrier security measures, there should be a financial incentive for carriers to protect their customers' phone calling records. The Commission should consider holding carriers individually and financially responsible for releasing CPNI to data vendors. Financial penalties are highly likely to result in meaningful data protection practices by carriers.

3. EPIC's Proposed Security Measures

The Commission seeks comment on EPIC's five proposals to address unauthorized means of obtaining CPNI. These are:

1. Consumer-set passwords
2. Audit trails
3. Encryption
4. Limiting data retention, and
5. Procedures for notice to the consumer on release of CPNI.

The five security measures recommended by EPIC represent a reasonable approach to stop unauthorized access to CPNI. Using the California Data Trace case as an example, the data broker would not have been able to obtain the phone records had a password been required. The illegal access would have been reported had the customer received notice of access. And, an audit trail would have allowed the carrier itself to take action against the data broker.

Encryption is another important security measure that carriers should be required to adopt in order to protect sensitive customer data from exploitation by hackers and others who are not authorized to have access to the information. Limiting data retention to the time necessary to handle billing questions is also a sensible precaution.

We urge the Commission to adopt rules to implement EPIC's recommended security measures. Such measures would not inconvenience customers in accessing their own records, and would significantly limit unauthorized access by others.

4. Existing Opt-Out Regime for Joint Partners

The Commission also seeks comment on whether the current opt-out regime sufficiently protections the privacy of CPNI when information is disclosed to carriers' joint venture partners and independent contractors. FCC rules now allow telephone companies to provide customer data to joint marketers without prior customer consent. Customers receive notice of the carrier's practices, but approval to share sensitive information with third parties is assumed unless the customer opts out within 30 days.

Privacy and consumer advocates have long argued against the opt-out strategy because it provides inadequate protection for sensitive data. Opt-out requires not only that the customer recognize the notice in the first instance, but also that the individual then assume the burden of following directions necessary to stop the flow of data. This is an easy way for companies to gain control of personal data since it is generally known that most consumers, under any negative option scheme, do not take the steps necessary to opt out.

With the current situation in which phone records are marketed on the Internet, it is important that consumers have maximum control over how personal information is used. Only an opt-in scheme requiring prior customer approval for all data sharing will provide adequate privacy protection.

We urge the Commission to reconsider its opt-out standard and, if needed, seek additional authority from Congress to set a higher standard. The Commission should replace the current opt-out with an opt-in that requires prior consent for any use of CPNI not directly related to the service for which the information was obtained.

5. Conclusion

We appreciate the opportunity for comment about the unacceptable practices that now allow private consumer telephone records to be offered for sale over the Internet. The Commission is warranted in finding this conduct disturbing and in granting EPIC's Petition for Rulemaking.

We urge the Commission to move swiftly to impose more stringent security standards upon carriers as its part in ending unauthorized access by data brokers, hackers, and others.

Sincerely,

Beth Givens, Director

Privacy Rights Clearinghouse
3100 5th Ave. #B
San Diego, CA 92103
www.privacyrights.org

Linda Sherry, Director of National Priorities
Consumer Action
PO Box 1762
Washington, DC 20013
www.consumer-action.org

Jean Ann Fox, Director of Consumer Protection
Consumer Federation of America
1620 Eye Street, NW, Suite 200
Washington, DC 20006
www.consumerfed.org

Richard Holober, Executive Director
Consumer Federation of California
520 S. El Camino Real, Suite 340
San Mateo, CA 94402
www.consumerfedofca.org

Jeannine Kenney, Senior Policy Analyst
Consumers Union
1666 Connecticut Ave. NW #310
Washington, DC 20009
www.consumersunion.org

Susan Grant, Vice President Public Policy
National Consumers League
1701 K Street NW, Suite 1200
Washington, DC 20006
www.nclnet.org

Linda Ackerman, Staff Counsel
PrivacyActivism
San Francisco, CA
www.privacyactivism.org

Michael Shames, Executive Director
Utility Consumers' Action Network
3100 5th Ave.
San Diego, CA 92103

www.ucan.org

---

[1] The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer education and advocacy organization based in San Diego, CA, established in 1992.

Consumer Action, founded in 1971, is a national nonprofit education and advocacy organization headquartered in San Francisco, CA, with offices in Washington, DC, and Los Angeles, CA.

Consumer Federation of America is a non-profit association of about 300 groups, with a combined membership of over 50 million people. CFA was founded in 1968 to advance the consumer interest through research, advocacy and education.

The Consumer Federation of California is a nonprofit advocacy organization, formed by its members to campaign for state and federal laws, and to appear before agencies, to protect consumers' rights. CFC also sponsors an Education Foundation which conducts education and research programs for consumers.

Consumers Union is a national nonprofit, independent organization that works on state and federal consumer policy issues with offices in Washington, DC; San Francisco, California; and Austin, Texas. The policy advocates testify before Federal and state legislative and regulatory bodies, petition government agencies, and file lawsuits on behalf of the consumer interest.

The National Consumers League was founded in 1899 to protect and promote social and economic justice for consumers and workers.

PrivacyActivism is a nonprofit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level.

The Utility Consumers' Action Network (UCAN), established in 1984, educates and protects San Diego County consumers in the areas of essential energy, utility, and telecommunications services.

[2] 71 *Federal Register* 13317, March 15, 2006

[3] Petition for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, submitted to the Federal Communications Commission by the Electronic Privacy Information Center (EPIC), www.epic.org/privacy/iei/cpnipet.html

[4] FTC Testifies on the Sale of Consumers' Phone Records, February 6, 2006, www.ftc.gov/opa/2006/02/pretexting060208.htm

[5] "State suing seller of cell phone records: Lawsuit asks for $10 million in civil penalties, restitution," Michael Kinsman, *San Diego Union Tribune*, March 15, 2006, www.signonsandiego.com/news/business/20060315-9999-1b15phone.html